ĐẠI HỌC QUỐC GIA HA NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

PHẠM HỮU TÙNG

ĐÁNH GIÁ HIỆU NĂNG BẢO MẬT TẦNG VẬT LÝ TRONG MẠNG NOMA

NGÀNH: MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG DỮ LIỆU
MÃ SỐ: 9480102

TÓM TẮT LUẬN ÁN TIẾN SĨ MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG DỮ LIỆU

Hà Nội - 2024

MỞ ĐẦU

1. Lý do lựa chọn đề tài

Trong những năm gần đây, sự phát triển mạnh mẽ của công nghệ mạng không dây đã mang lại cho con người cơ hội tiếp cận nhiều loại hình dịch vụ, tiện ích khác nhau. Tuy nhiên, cùng với sự phát triển của công nghệ mạng không dây cộng thêm với đặc tính tự nhiên của truyền thông không dây như tính mở, tính quảng bá, v.v. đã làm gia tăng các hoạt động bất hợp pháp trên mạng. Do đó đảm bảo truyền thông an toàn là một trong những yêu cầu cấp thiết trong quá trình thiết kế các hệ thống truyền thông không dây.

Giải pháp bảo mật để chống lại các hoạt động bất hợp pháp ở trên là dựa theo cách tiếp cận từng lớp của mô hình tham chiếu kết nối các hệ thống mở (OSI). Trong đó, theo phương pháp truyền thống đã áp dụng ở các lớp trên tầng vật lý như dụng thuật toán mã hóa nâng cao (AES), thuật toán mã hóa khóa công khai (RSA) ở tầng ứng dụng. Các giải pháp bảo mật này có ưu điểm thực hiện bảo mật trực tiếp và đang được sử dụng phổ biến trong các hệ thống thông tin hiện nay. Tuy nhiên, với sự phát triển mạnh mẽ về năng lực tính toán của các hệ thống máy tính thì các phương pháp bảo mật dựa trên thời gian tính toán và bộ nhớ cần thiết để phá mã có thể không còn phù hợp trong tương lai khi năng lực tính toán của hệ thống máy tính bẻ khóa ngày càng cao và có khả năng không còn bị giới hạn. Mặc khác, phương pháp bảo mật dựa trên độ phức tạp của thuật toán mã hóa, gặp nhiều khó khăn, hạn chế trong việc quản lý và phân phối khóa đối với các mô hình mạng phân tán, và là thách thức lớn đối với các thiết bị trong mạng Internet vạn vật (IoT) vốn có tài nguyên hạn chế.

Để giải quyết vấn đề trên, các nhà nghiên cứu cả trong và ngoài nước đã tập trung nghiên cứu đưa ra các giải pháp bảo mật lớp vật lý (PLS)

dựa trên cơ sở lý thuyết thông tin do Shannon đề xuất từ năm 1948. Bảo mật tầng vật lý không dựa trên độ phức tạp tính toán, có nghĩa là mức độ bảo mật đạt được sẽ không bị vượt qua ngay cả khi các thiết bị bất hợp pháp có năng lực tính toán mạnh mẽ.

Mạng đa truy cập không trực giao (NOMA) là một công nghệ tiềm năng cho mạng thế hệ thứ 5 và tương lai, nó cho phép đồng thời nhiều người dùng cùng truy cập dựa trên cơ chế sử dụng chung khối tài nguyên không trực giao trong mạng vô tuyến như cùng khe thời gian, cùng tần số,v.v., trái ngược với cơ chế hoạt động của hệ thống đa truy cập trực giao thường dựa trên chia sẻ tài nguyên trực giao.

Với sự phổ biến và phát triển không ngừng của công nghệ mạng không dây, vấn đề bảo mật trong truyền thông không dây sẽ có nhiều thách thức hơn nữa trong tương lai, làm cho chủ đề này trở thành một trong những lĩnh vực nghiên cứu quan trọng và liên tục. Mặc dù đã có nhiều các công trình nghiên cứu với cách tiếp cận khác nhau, song truyền thông bảo mật trong mạng NOMA vẫn đang là một vấn đề mở. Do đó luận án đề xuất các mô hình mạng NOMA với các kỹ thuật truyền thông tiên tiến như chủ động gây nhiễu, đa ăng-ten, truyền thông cộng tác kết hợp với các kỹ thuật lựa chọn ăng-ten phát (TAS), lựa chọn kết hợp (SC). Sau đó thực hiện phân tích, đánh giá hiệu năng bảo mật hệ thống, góp phần mở rộng thêm các kết quả nghiên cứu cũng như làm phong phú và sáng tỏ sự hiểu biết về bảo mật thông tin tầng vật lý trong mạng NOMA. Đây là vấn đề quan trọng, cấp thiết và chính là mục tiêu nghiên cứu của luận án.

2. Mục tiêu nghiên cứu

Mục tiêu của luận án là nghiên cứu, đánh giá và đề xuất giải pháp nhằm nâng cao khả năng bảo mật thông tin tại tầng vật lý trong mạng NOMA, nhằm ngăn chặn hình thức tấn công nghe lén thông tin và đảm bảo QoS cho hệ thống. Luận án gồm các mục tiêu cụ thể sau:

- Đề xuất các mô hình mạng NOMA sử dụng các kỹ thuật truyền thông tiên tiến như truyền thông cộng tác, vô tuyến nhận thức, gây nhiễu cộng tác.

- Phân tích, đánh giá khả năng đảm bảo an toàn thông tin tầng vật lý, đề xuất các chiến lược nâng cao khả năng bảo mật và phân tích hiệu quả bảo mật của chiến lược được đề xuất trên kênh truyền Rayleigh fading và $\alpha - \mu$ fading.
- Xây dựng biểu thức toán học, chương trình mô phỏng để đánh giá tác động của các tham số hệ thống lên hiệu năng bảo mật của hệ thống.

3. Các đóng góp chính của luận án

Những đóng góp chính của luận án được tóm tắt như sau:

- Một là đã đề xuất và đánh giá chiến lược bảo mật thông tin cho mạng NOMA cộng tác trên kênh truyền α-μ fading bị thiết bị gây nhiễu và nghe lén hợp tác tấn công thông qua phép đo xác suất dừng bảo mật trong kịch bản hệ thống có chiến lược đối phó chủ động và không có chiến lược đối phó chủ động. Các kết quả mô phỏng đã chỉ ra rằng hiệu năng bảo mật của hệ thống được cải thiện đáng kể trong kịch bản có chiến lược đối phó chủ động. Kết quả này được công bố trong công trình số $A1$.
- Hai là đã đề xuất và đánh giá hiệu năng bảo mật của mô hình mạng NOMA có chiến lược nghe lén chủ động dựa trên các biểu thức dạng đóng của phép đo xác suất nghe lén hợp pháp thành công, xây dựng một chính sách điều chỉnh công suất truyền tin trong kịch bản trạng thái kênh truyền xác định và không xác định vừa đảm bảo hiệu suất nghe lén vừa thỏa mãn ràng buộc về xác suất dừng hoạt động của hệ thống truyền tin bất hợp pháp. Các kết quả phân tích lý thuyết và mô phỏng chỉ ra rằng hiệu năng bảo mật của hệ thống tăng đáng kể khi số lượng ăng-ten của thiết bị chuyển tiếp tăng lên. Kết quả này được công bố trong công trình số $A3$.
- Ba là đã đề xuất và đánh giá khả năng bảo mật thông tin mô hình mạng SISO NOMA với các kịch bản khác nhau về thiết bị nghe lén Eve. Hiệu năng bảo mật được phân tích, đánh giá thông qua phép

đo xác suất dừng bảo mật của từng người dùng, của toàn bộ hệ thống với kịch bản Eve sử dụng các kỹ thuật SIC, PIC để xử lý tín hiệu thu được, kịch bản Eve được trang bị một và nhiều ăng-ten. Các kết quả phân tích lý thuyết và mô phỏng đã chỉ ra rằng hiệu năng bảo mật của hệ thống trong trường hợp Eve sử dụng PIC kém hơn so với trường hợp Eve sử dụng kỹ thuật SIC. Hơn nữa, hệ thống sẽ bảo mật hơn khi Eve chỉ được trang bị một ăng-ten so với trường hợp thiết bị nghe lén được trang bị nhiều ăng-ten. Kết quả này được công bố trong công trình số $A2$.

- Bốn là đã khảo sát, đánh giá được mối quan hệ giữa khả năng bảo mật thông tin và độ tin cậy của mô hình mạng NOMA nhận thức dưới ràng buộc mức can nhiễu của mạng sơ cấp và công suất phát tối đa của mạng thứ cấp. Các kết quả đã chỉ ra rằng giữa bảo mật và độ tin cậy có mối quan hệ tỷ lệ nghịch. Đồng thời đưa ra chính sách điều chỉnh công suất của mạng thứ cấp để vừa đảm bảo an toàn thông tin của mạng thứ cấp vừa đảm bảo hiệu suất hoạt động của mạng sơ cấp. Hiệu năng của hệ thống được đánh giá dựa trên các biểu thức dạng đóng của các phép đo xác suất dừng hệ thống và xác suất bị nghe lén. Kết quả này được công bố trong công trình số $A4$.

4. Cấu trúc của luận án

Luận án được bố cục bao gồm các phần như sau: Mở đầu, 04 chương, Kết luận và định hướng nghiên cứu, Phụ lục, Danh mục công trình khoa học và Tài liệu tham khảo.

Phần mở đầu: Tập trung làm rõ các lý do lựa chọn đề tài nghiên cứu, xác định rõ mục tiêu, đối tượng, phạm vi nghiên cứu, phương pháp nghiên cứu, các đóng góp chính của luận án, ý nghĩa khoa học và thực tiễn của luận án.

Chương 1: Trình bày tổng quan về những vấn đề nghiên cứu.

Chương 2: Phân tích, đánh giá hiệu năng bảo mật mạng NOMA có chiến lược đối phó chủ động với hình thức tấn công hợp tác.

Chương 3: Đề xuất và đánh giá hiệu năng bảo mật mạng NOMA có chiến lược chủ động nghe lén dựa trên phép đo xác suất nghe lén hợp pháp thành công.

Chương 4: Nghiên cứu, so sánh và phân tích hiệu năng bảo mật mô hình mạng SISO NOMA, khảo sát sự đánh đổi giữa giữa bảo mật và độ tin cậy mạng NOMA nhận thức dạng nền dưới ràng buộc mức can nhiễu của mạng thứ cấp và công suất phát mức đỉnh.

Phần kết luận và định hướng nghiên cứu của luận án sẽ trình bày tóm lược những kết quả nghiên cứu, những đóng góp của luận án đã được công bố các trên tạp chí và các hội thảo khoa học. Đồng thời đề xuất các hướng nghiên cứu tiếp theo của luận án.

Chương 1

KIẾN THỨC CƠ SỞ VÀ TỔNG QUAN

1.1 Mạng NOMA

Các nhà nghiên cứu đề xuất NOMA như một ứng cử viên sáng giá về kỹ thuật đa truy cập cho các thế hệ tiếp theo để cải thiện hiệu quả phổ đồng thời cho phép nhiễu đa truy nhập ở một mức độ nào đó tại các máy thu.

1.2 Bảo mật lớp vật lý trong mạng NOMA

1.2.1 Cơ sở lý thuyết bảo mật tầng vật lý

Phương pháp bảo mật lớp vật lý được khởi xướng bởi Wyner từ năm 1975. Cơ sở lý thuyết bảo mật thông tin tầng vật lý xuất phát từ khái niệm bảo mật hoàn hảo (perfect secrecy) và lý thuyết thông tin đưa ra bởi Shannon vào năm 1949.

1.2.2 Phép đo hiệu năng bảo mật hệ thống

Hiệu năng bảo mật của hệ thống mạng không dây trên các kênh fading được đánh giá chủ yếu thông qua các phép đo: *Dung lượng bảo mật*, *xác*

suất dừng bảo mật, *xác suất nghe lén hợp pháp thành công*, *xác suất bị nghe lén*, và *thông lượng bảo mật*.

1.2.2.1 Dung lượng bảo mật kênh

Các nghiên cứu về bảo mật lớp vật lý trong mạng không dây xác định dung lượng bảo mật kênh là sự khác biệt giữa dung lượng kênh của kênh hợp pháp và dung lượng kênh nghe lén. Do tính chất không âm của dung lượng kênh, dung lượng bảo mật biểu diễn như sau

$$C_s = \begin{cases} \log_2(1+\gamma_m) - \log_2(1+\gamma_e), & \text{nếu } \gamma_m > \gamma_e \\ 0, & \text{nếu } \gamma_m \leq \gamma_e \end{cases} \tag{1.1}$$

trong đó γ_m, và γ_e lần lượt là SNR của kênh hợp pháp và kênh nghe lén, tương ứng. Theo (1.1), có thể thấy rằng dung lượng bảo mật kênh lớn hơn 0 khi $\gamma_m > \gamma_e$. Vì vậy, một trong những nội dung quan trọng trong đánh giá khả năng bảo mật của hệ thống là tính toán xác suất tồn tại một dung lượng bảo mật kênh lớn hơn 0.

1.2.2.2 Xác suất dừng bảo mật

Gọi $R_s > 0$ là tốc độ bảo mật mong muốn của hệ thống. Xác suất dừng bảo mật của hệ thống là xác suất mà dung lượng bảo mật tức thời C_s nhỏ hơn giá trị của R_s, nghĩa là

$$\mathcal{O}_{sec} = Pr(C_s < R_s) \tag{1.2}$$

1.2.3 So sánh bảo mật dùng mã mật với bảo mật tầng vật lý

Bảo mật lớp vật lý chưa được hoàn thiện và chưa được ứng dụng nhiều trong thực tế, tuy nhiên các đặc điểm khác biệt của bảo mật lớp vật lý so với bảo mật dùng mật mã đã thu hút sự quan tâm của các nhà nghiên cứu trên khắp thế giới.

Chương 2

ĐÁNH GIÁ HIỆU NĂNG BẢO MẬT MẠNG NOMA CỘNG TÁC CÓ CHIẾN LƯỢC ĐỐI PHÓ CHỦ ĐỘNG VỚI HÌNH THỨC TẤN CÔNG HỢP TÁC

2.1 Mô hình hệ thống

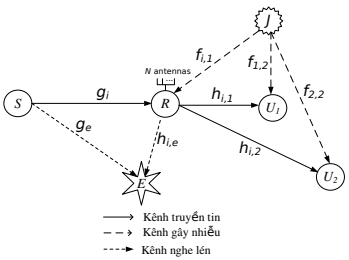
Nguồn S truyền tín hiệu đồng thời đến cả U_1 và U_2 với sự hỗ trợ của thiết bị chuyển tiếp R sử dụng giao thức giải mã và chuyển tiếp, có hai thiết bị hoạt động bất hợp pháp, một thiết bị gây nhiễu J và một thiết bị nghe lén E. Giải thiết rằng S, U_1, U_2, và E được trang bị đơn ăng-ten, thiết bị chuyển tiếp R được trang bị N ăng-ten.

2.1.1 Kịch bản hệ thống không có chiến lược đối phó chủ động

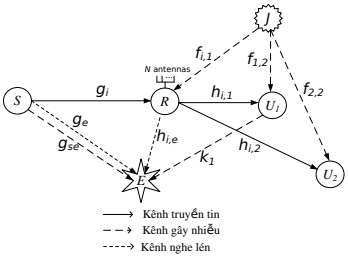
Biểu thức tỉ số SNR và SINR tại E như sau

$$\gamma_e^{s_1} = \max\left\{\gamma_{s_1,e}^{(1)}, \gamma_{s_1,e}^{(2)}\right\}, \tag{2.1}$$

$$\gamma_e^{s_2} = \max\left\{\gamma_{s_2,e}^{(1)}, \gamma_{s_2,e}^{(2)}\right\}. \tag{2.2}$$



Hình 2.1: *Mô hình mạng NOMA cộng tác không sử dụng chiến lược đối phó chủ động với hình thức tấn công hợp tác*



Hình 2.2: *Mô hình mạng NOMA cộng tác có sử dụng chiến lược đối phó chủ động với hình thức tấn công hợp tác*

2.1.2 Kịch bản hệ thống có chiến lược đối phó chủ động

Biểu thức tỉ số SINR của tín hiệu s_1 và s_2 mà E nghe lén được như sau

$$\gamma_{ej}^{s_1} = \max\left\{\gamma_{s_1,ej}^{(1)}, \gamma_{s_1,ej}^{(2)}\right\}, \tag{2.3}$$

$$\gamma_{ej}^{s_2} = \max\left\{\gamma_{s_2,ej}^{(1)}, \gamma_{s_2,ej}^{(2)}\right\}. \tag{2.4}$$

2.2 Phân tích xác suất dừng bảo mật

2.2.1 Xác suất dừng bảo mật trong kịch bản hệ thống không có chiến lược đối phó chủ động

Xác suất dừng bảo mật của hệ thống trong kịch bản không có chiến lược đối phó chủ động xảy ra khi dung lượng bảo mật người dùng U_1 hoặc U_2 nhỏ hơn ngưỡng quy định tương ứng

$$\mathcal{O}_{sec}^{NPS} = \Pr\left\{C_s^{1,NPS} < R_1 \ \ or \ \ C_s^{2,NPS} < R_2\right\} \tag{2.5}$$

$$= \Pr\left\{\gamma^{s_1} < \delta_1 + (\delta_1+1)\gamma_e^{s_1} \right.$$
$$\left. or \ \ \gamma^{s_2} < \delta_2 + (\delta_2+1)\gamma_e^{s_2}\right\}, \tag{2.6}$$

trong đó $\delta_1 = 2^{\frac{2R_1}{B}} - 1$ và $\delta_2 = 2^{\frac{2R_2}{B}} - 1$.

2.2.2 Xác suất dừng bảo mật trong kịch bản hệ thống có chiến lược đối phó chủ động

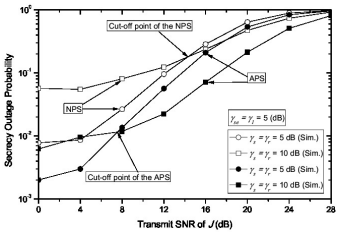
Xác suất dừng bảo mật của hệ thống trong kịch bản có chiến lược đối phó chủ động xảy ra khi dung lượng bảo mật người dùng U_1 hoặc U_2 nhỏ hơn ngưỡng quy định tương ứng

$$\begin{aligned}\mathcal{O}_{sec}^{APS} &= \Pr\left\{C_s^{1,APS} < R_1 \ \ or \ \ C_s^{2,APS} < R_2\right\} \\ &= \Pr\left\{\gamma^{s_1} < \delta_1 + (\delta_1+1)\gamma_{ej}^{s_1} \right. \qquad (2.7) \\ &\qquad\qquad or \ \ \gamma^{s_2} < \delta_2 + (\delta_2+1)\gamma_{ej}^{s_2}\Big\}. \qquad (2.8)\end{aligned}$$

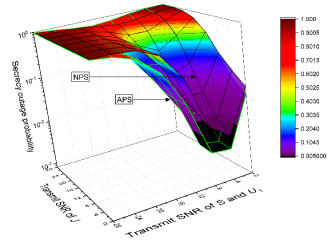
2.3 Mô phỏng và đánh giá kết quả

Kết quả mô phỏng cho thấy rằng SOP trong kịch bản APS thấp hơn đáng kể so với kịch bản NPS trên toàn bộ miền giá trị SNR của thiết bị gây nhiễu. Điều này được giải thích như sau, S và U_1 được sử dụng như là nút gây nhiễu thân thiện để làm suy giảm tín hiệu nghe lén tại E trong kịch bản APS. Hơn thế nữa, khi SNR của J giảm thì SOP của hệ thống trong cả hai kịch bản đều được cải thiện bởi vì SINR để giải mã các tín hiệu s_1 và s_2 tại R, U_1, U_2 chịu ảnh hưởng tiêu cực từ tín hiệu nhiễu gây ra bởi J.

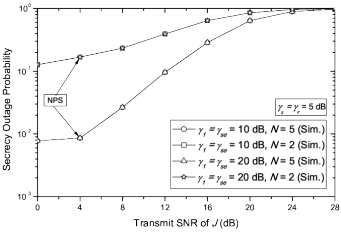
Công suất SNR của thiết bị gây nhiễu thân thiện S và U_1 khi tăng từ $\gamma_{se} = \gamma_1 = 10$ dB đến $\gamma_{se} = \gamma_1 = 20$ dB, SOP trong kịch bản APS giảm đáng kể trong khi ở kịch bản NPS thì không thay đổi. Hiện tượng trên xảy ra bởi vì trong kịch bản NPS hệ thống không có bất kỳ chiến lược nào để bảo vệ hệ thống, ngược lại trong kịch bản APS hệ thống sử dụng S và U_1 như là hai nút gây nhiễu thân thiện để làm suy yếu tín hiệu nghe lén tại E. Hơn nữa, SOP của hệ thống trong cả hai kịch bản được cải thiện khi số lượng ăng-ten của nút nguồn tăng lên. Nguyên nhân là do khi số lượng ăng-ten tăng lên thì độ lợi phân tập (diversity gain) tại nút nguồn cũng tăng lên.



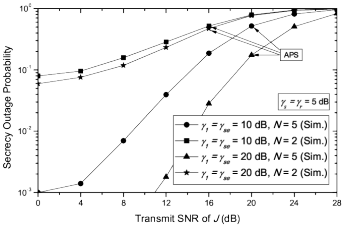
Hình 2.3: *Tác động của SNR tại J, S, và R lên SOP trong kịch bản NPS và APS với* $\alpha = 2$, $\mu = 1, \Omega_{g_i} = \Omega_{h_{i,1}} = \Omega_{h_{i,2}} = \Omega_{k_1} = 5$, *và* $\Omega_{g_e} = \Omega_{g_{s,e}} = \Omega_{h_{i,e}} = \Omega_{f_{i,1}} = \Omega_{f_{1,2}} = \Omega_{f_{2,2}} = 0.1$.



Hình 2.4: *Tác động của SNR tại J, S, và R lên SOP trong kịch bản NPS và APS với* $\alpha = 2$, $\mu = 1, \Omega_{g_i} = \Omega_{h_{i,1}} = \Omega_{h_{i,2}} = \Omega_{k_1} = 5$, *và* $\Omega_{g_e} = \Omega_{g_{s,e}} = \Omega_{h_{i,e}} = \Omega_{f_{i,1}} = \Omega_{f_{1,2}} = \Omega_{f_{2,2}} = 0.1$.



Hình 2.5: *Tác động của số lượng ăng-ten tại R và SNR tại J, S, và* U_1 *lên SOP trong kịch bản NPS với* $\alpha = 2$, $\mu = 1$, $\Omega_{g_i} = \Omega_{h_{i,1}} = \Omega_{h_{i,2}} = \Omega_{k_1} = 5$ *và* $\Omega_{g_e} = \Omega_{g_{se}} = \Omega_{h_{i,e}} = \Omega_{f_{1,2}} = \Omega_{f_{2,2}} = \Omega_{f_{i,1}} = 0.1$.



Hình 2.6: *Tác động của số lượng ăng-ten của R và SNR của J, S, và* U_1 *lên SOP trong kịch bản APS với* $\alpha = 2$, $\mu = 1$, $\Omega_{g_i} = \Omega_{h_{i,1}} = \Omega_{h_{i,2}} = \Omega_{k_1} = 5$ *và* $\Omega_{g_e} = \Omega_{g_{se}} = \Omega_{h_{i,e}} = \Omega_{f_{1,2}} = \Omega_{f_{2,2}} = \Omega_{f_{i,1}} = 0.1$.

Chương 3

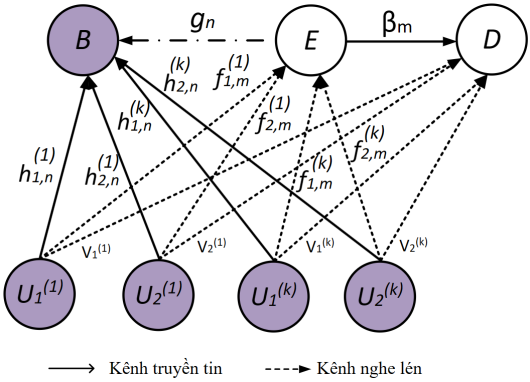
ĐÁNH GIÁ HIỆU NĂNG BẢO MẬT MẠNG NOMA CÓ CHIẾN LƯỢC CHỦ ĐỘNG NGHE LÉN

3.1 Mô hình hệ thống

Trong chương này, luận án khảo sát một mô hình mạng NOMA như hình 3.1. Hệ thống bao gồm một trạm thu, phát sóng bất hợp pháp B được trang bị N ăng-ten, 2K thiết bị đầu cuối bất hợp pháp $U = \{U^{(1)}, ..., U^{(2K)}\}$, được nghép lại thành từng đôi một ngẫu nhiên $U_l^{(k)}$, $l \in \{1, 2\}$ và $k \in \{1, 2, \ldots, K\}$, mỗi thiết bị được trang bị một ăng-ten, một thiết bị điều khiển hợp pháp được trang bị $M + 1$ ăng-ten, thiết bị nhận hợp pháp D được trang bị một ăng-ten. Mỗi cặp $U_l^{(k)}$ sử dụng kỹ thuật NOMA để truyền tín hiệu về trạm thu sóng B và giả định $U_1^{(k)}$ gần B hơn so với $U_2^{(k)}$.

3.2 Chính sách phân bổ công suất gây nhiễu

Công suất truyền tin P_s của cặp thiết bị $U_l^{(k)}$ và công suất gây nhiễu P_J của E trong thực tế phải thỏa mãn ràng buộc nhỏ hơn hoặc bằng công suất tối đa hay còn gọi là công suất mức đỉnh, do đó công suất gây nhiễu



Hình 3.1: *Mô hình mạng NOMA có chiến lược chủ động nghe lén.*

sẽ là

$$0 \leq P_J \leq P_J^{max}, 0 \leq P_s \leq P_s^{max}. \tag{3.1}$$

3.2.1 Trạng thái kênh gây nhiễu là xác định

Miền giá trị công suất P_J dưới ràng buộc xác suất dừng hoạt động của $U_2^{(k)}$ và công suất gây nhiễu tối đa của E được xác định như sau

$$P_J \leq \min\left\{P_{J_2}, P_J^{max}\right\}. \tag{3.2}$$

$$0 \leq P_J \leq \min\left\{\min\left\{P_{J_1}, P_{J_2}\right\}, P_J^{max}\right\}. \tag{3.3}$$

3.2.2 Trạng thái kênh gây nhiễu không xác định

Miền giá trị của công suất tín hiệu nhiễu của E trong trường hợp trạng thái kênh truyền không xác định như sau

$$0 \leq P_J \leq \min\left\{\min\left\{P_{J_1^*}, P_{J_2^*}\right\}, P_J^{max}\right\}. \tag{3.4}$$

3.3 Xác suất nghe lén hợp pháp thành công

3.3.1 Xác suất nghe lén hợp pháp thành công đối với thiết bị đầu cuối có tín hiệu mạnh nhất

Xác suất nghe lén thành công đối với người dùng có tín hiệu mạnh nhất được tính toán theo công thức sau

$$\mathcal{O}_{suc}^{(1)} = \Pr\left\{\max_{k\in\{1,2,\ldots,K\}}\left\{R_{1,E2E}^{(k)}\right\} \geq r_1\right\}, \tag{3.5}$$

trong đó $R_{1,E2E}^{(k)}$ là tỷ số tín hiệu trên nhiễu người dùng có tín hiệu mạnh nhất.

3.3.2 Xác suất nghe lén hợp pháp thành công đối với thiết bị đầu cuối có tín hiệu yếu nhất

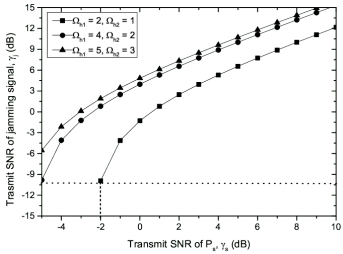
Xác suất nghe lén thành công cho người dùng có tín hiệu yếu nhất được mô tả bởi biểu thức sau

$$\mathcal{O}_{suc}^{(2)} = \Pr\left\{\min_{k\in\{1,2,\ldots,K\}}\left\{R_{2,E2E}^{(k)}\right\} \geq r_2\right\}, \tag{3.6}$$

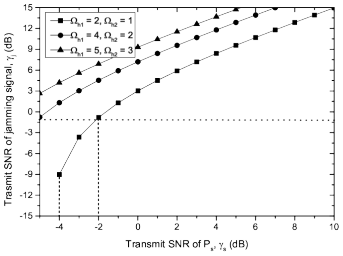
trong đó $R_{2,E2E}^{(k)}$ là tỷ số tín hiệu trên nhiễu người dùng có tín hiệu yếu nhất.

3.4 Mô phỏng và đánh giá kết quả

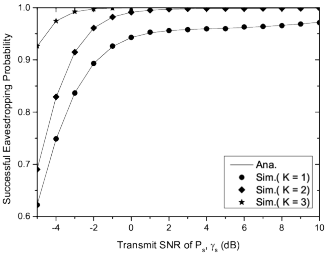
Xác suất nghe lén hợp pháp thành công cho cả người dùng có tín hiệu mạnh nhất và yếu nhất đều tăng khi số lượng ăng-ten của E tăng. Điều này xảy ra do khi số lượng ăng-ten của E tăng lên thì độ lợi phân tập tại E cũng tăng lên. Điều này cho thấy tăng số lượng ăng-ten tại E là cách đơn giản và hiệu quả để cải thiện xác suất nghe lén hợp pháp, việc tăng số lượng ăng-ten dễ dàng thực hiện được trong mạng 5G vì công nghệ mạng 5G hỗ trợ các thiết bị đa ăng-ten.



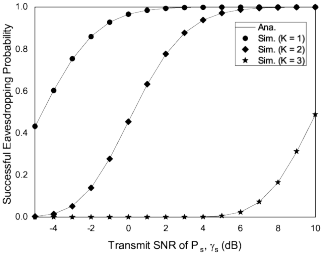
Hình 3.2: *SNR của tín hiệu nhiễu trong trường hợp kênh truyền gây nhiễu E→B xác định và* $\Omega_{g_n} = 1$



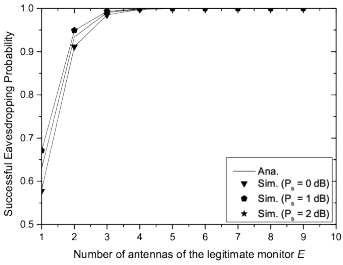
Hình 3.3: *SNR của tín hiệu nhiễu trong trường hợp kênh truyền gây nhiễu E→B không xác định và* $\Omega_{g_n} = 1$



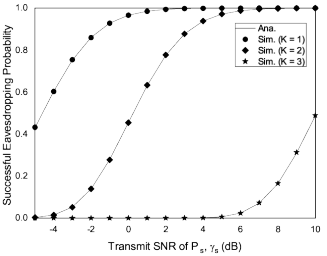
Hình 3.4: *Tác động của số lượng cặp người dùng lên* $\mathcal{O}_{suc}^{(1)}$ *theo tập giá trị của* γ_s



Hình 3.5: *Tác động của số lượng cặp người dùng lên* $\mathcal{O}_{suc}^{(2)}$ *theo tập giá trị của* γ_s



Hình 3.6: *Tác động của số lượng ăng-ten lên* $\mathcal{O}_{suc}^{(1)}$ *theo tập giá trị của* γ_s



Hình 3.7: *Tác động của số lượng ăng-ten lên* $\mathcal{O}_{suc}^{(2)}$ *theo tập giá trị của* γ_s

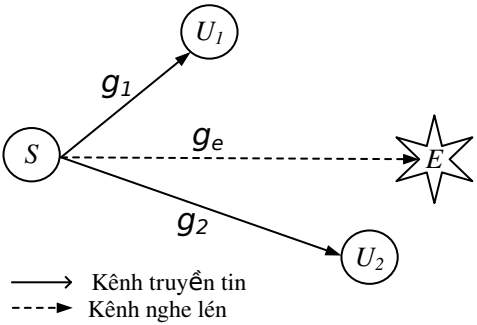
Chương 4

ĐÁNH GIÁ HIỆU NĂNG BẢO MẬT, ĐỘ TIN CẬY MẠNG SISO NOMA VÀ MẠNG NOMA NHẬN THỨC

4.1 Mô hình 4.1: Đánh giá hiệu năng bảo mật và tính công bằng thời gian truyền tin mạng SISO NOMA

4.1.1 Mô hình hệ thống

Mô hệ thống NOMA như được mô tả trong hình 4.1, trong đó BS đồng thời truyền tin đến hai người dùng cuối là U_1 và U_2, cùng thời điểm đó thiết bị nghe lén Eve đồng thời hiện diện thực hiện việc thu thập thông tin bất hợp pháp.



Hình 4.1: *Mô hình mạng NOMA có một trạm cơ sở BS, hai người dùng cuối, và một nút nghe lén Eve. Người dùng U_1 gần BS hơn so với U_2.*

4.1.2 Phân tích hiệu năng bảo mật trong kịch bản Eve có một ăng-ten

4.1.2.1 Xác suất dừng bảo mật trong kịch bản Eve sử dụng kỹ thuật loại bỏ nhiễu SIC

4.1.2.2 Xác suất dừng bảo mật của người dùng

Biểu thức xác suất dừng bảo mật của U_1

$$\mathcal{O}_{sec}^{U_1,SIC} = 1 - \frac{\lambda_{e_1} \exp\left(-\lambda_1 \delta_1\right)}{\lambda_1(\delta_1 + 1) + \lambda_{e_1}}. \tag{4.1}$$

Biểu thức xác suất dừng bảo mật của U_2

$$\mathcal{O}_{sec}^{U_2,SIC} = 1 - \lambda_2 \alpha_2 (I_1 - I_2). \tag{4.2}$$

4.1.2.3 Xác suất dừng bảo mật của hệ thống

Biểu thức xác suất dừng bảo mật của hệ thống

$$\mathcal{O}_{sec}^{SIC} = 1 - \frac{1}{\Omega_e} \int_0^{\rho} \exp\left(-\frac{F_1(x)}{\Omega_1} - \frac{F_2(x)}{\Omega_2} - \frac{x}{\Omega_e}\right) dx \tag{4.3}$$

4.1.2.4 Xác suất dừng bảo mật trong kịch bản Eve sử dụng kỹ thuật loại bỏ nhiễu PIC

4.1.2.5 Xác suất dừng bảo mật của người dùng

Biểu thức xác suất dừng bảo mật của U_2

$$\mathcal{O}_{sec}^{U_2,PIC} = 1 - \lambda_2 \alpha_2 (I1 - I3), \tag{4.4}$$

4.1.2.6 Xác suất dừng bảo mật của hệ thống

Biểu thức xác suất dừng bảo mật của hệ thống

$$\mathcal{O}_{sec}^{PIC} = 1 - K \int_0^{\epsilon} \exp(\psi) dx, \tag{4.5}$$

4.1.3 Phân tích hiệu năng bảo mật trong kịch bản Eve có nhiều ăng-ten

4.1.3.1 Xác suất dừng bảo mật hệ thống trong kịch bản Eve sử dụng kỹ thuật loại bỏ nhiễu SIC

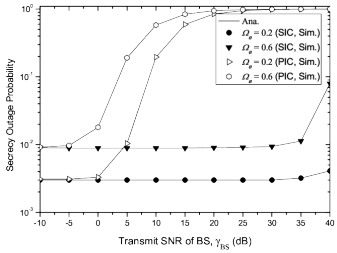
Biểu thức xác suất dừng bảo mật của hệ thống

$$\mathcal{O}_{sec}^{(N,SIC)} = 1 - N * K \int_0^{\rho} \exp(\chi) \nu dx, \tag{4.6}$$

4.1.3.2 Xác suất dừng bảo mật hệ thống trong kịch bản Eve sử dụng kỹ thuật loại bỏ nhiễu PIC

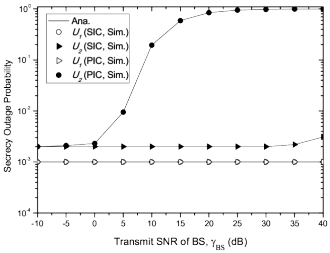
Biểu thức xác suất dừng bảo mật của hệ thống

$$\mathcal{O}_{sec}^{(N,PIC)} = 1 - N * K \int_0^{\epsilon} \exp(\pi) \nu dx, \tag{4.7}$$

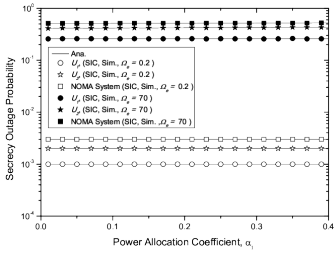


Hình 4.2: *SOP của hệ thống theo tập giá trị SNR trong kịch bản Eve sử dụng kỹ thuật loại bỏ nhiễu SIC và PIC với* $\Omega_1 = 200, \Omega_2 = 100,$ *và* $\alpha_1 = 0.3$.

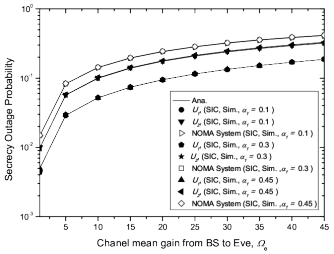
.



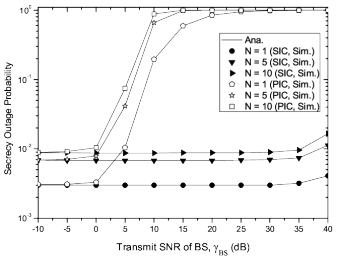
Hình 4.3: *SOP của* U_1 *và* U_2 *theo tập giá trị SNR trong kịch bản Eve sử dụng kỹ thuật loại bỏ nhiễu SIC và PIC với* $\Omega_1 = 200, \Omega_2 = 100, \Omega_e = 0.2,$ *và* $\alpha_1 = 0.3$.



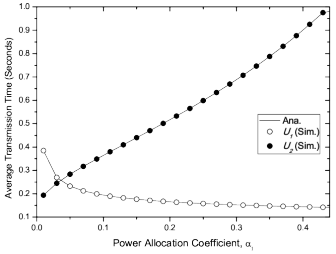
Hình 4.4: *SOP của hệ thống theo miền giá trị của hệ số phân bổ công suất* α_1 *trong kịch bản Eve sử dụng kỹ thuật SIC với* $\Omega_1 = 200, \Omega_2 = 100, \Omega_e = 0.2,$ *và SNR = 10 dB.*



Hình 4.5: *SOP của hệ thống theo miền giá trị độ lợi kênh truyền trong kịch bản Eve sử dụng kỹ thuật SIC với* $\Omega_1 = 200, \Omega_2 = 100,$ *và SNR = 10 dB.*



Hình 4.6: *Tác động của số lượng ăng-ten lên $\mathcal{O}_{suc}^{(1)}$ theo tập giá trị của γ_S*



Hình 4.7: *Tác động của số lượng ăng-ten của Eve lên SOP của hệ thống với $\Omega_1 = 200, \Omega_2 = 100, \Omega_e = 2$.*

4.1.4 Mô phỏng và phân tích kết quả

4.2 Mô hình 4.2: Đánh giá hiệu năng bảo mật và độ tin cậy mạng NOMA nhận thức dạng nền dưới ràng buộc mức can nhiễu của mạng sơ cấp

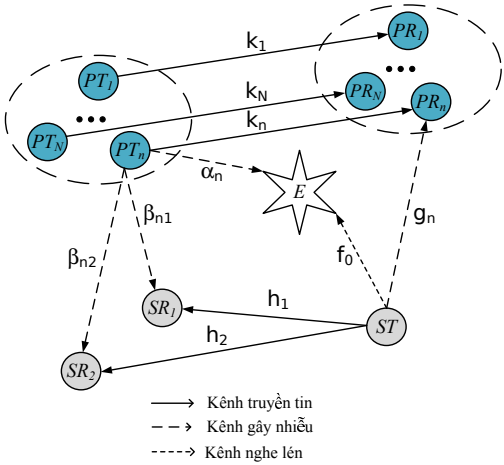
4.2.1 Mô hình hệ thống

4.2.2 Phân tích hiệu suất hệ thống

4.2.2.1 Ràng buộc về công suất của mạng thứ cấp

Mạng thứ cấp thiết lập công suất phát dựa hoàn toàn vào ràng buộc can nhiễu của mạng sơ cấp, được mô tả bằng toán học như sau:

$$0 \leq P_s \leq \min\left\{P_I, P_s^{max}\right\}. \tag{4.8}$$



Hình 4.8: *Mô hình mạng NOMA nhận thức dưới ràng buộc mức can nhiễu của mạng sơ cấp*

4.2.2.2 Xác suất bị nghe lén

Xác suất thông tin mạng thứ cấp bị E nghe lén được biểu diễn như sau:

$$\mathcal{O}_{int} = \Pr\left\{C_{Eve}^{(1)} > \theta_{th}^{(1)} \; or \; C_{Eve}^{(2)} > \theta_{th}^{(2)}\right\}. \tag{4.9}$$

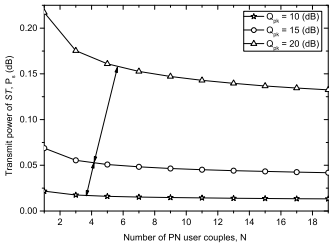
4.2.2.3 Xác suất dừng hệ thống

Trong mô hình này, mạng thứ cấp dừng truyền tin khi dung lượng kênh truyền từ ST đến SR_1 và SR_2 nằm dưới ngưỡng được xác định cho trước tương ứng của R_1 và R_2

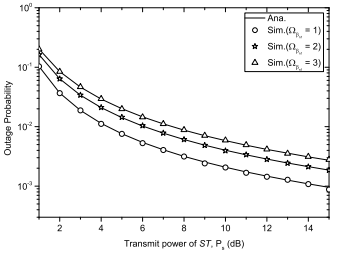
$$\mathcal{O}_{out} = \Pr\left\{C^{(1)} < R_1 \; or \; C^{(2)} < R_2\right\}. \tag{4.10}$$

4.2.3 Mô phỏng và đánh giá kết quả

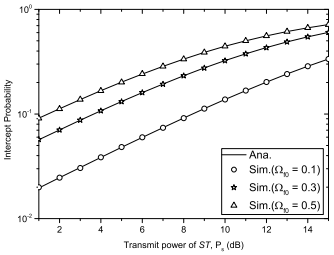
Chúng ta có thể quan sát thấy khi xác suất dừng hệ thống tăng lên thì xác suất bị nghe lén giảm xuống, và ngược lại.



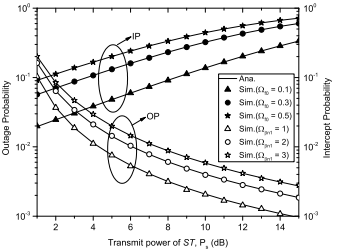
Hình 4.9: *Mối quan hệ giữa công suất phát của mạng thứ cấp và số cặp người dùng của mạng sơ cấp.*



Hình 4.10: *Mối quan hệ giữa xác suất dừng hoạt động với công suất phát của của mạng thứ cấp.*



Hình 4.11: *Xác suất mạng thứ cấp bị nghe lén so với công suất phát của mạng thứ cấp*



Hình 4.12: *Mối quan hệ giữa xác suất dừng hoạt động, xác suất bị nghe lén của mạng thứ cấp so với công suất phát của mạng thứ cấp P_s*

KẾT LUẬN

Các kết quả đóng góp mới về khoa học của Luận án bao gồm:

1. Luận án đã phân tích làm rõ các khái niệm mạng NOMA, bảo mật tầng vật lý, cơ sở lý thuyết của kỹ thuật bảo mật tầng vật lý, so sánh ưu nhược điểm của kỹ thuật bảo mậng tầng vật lý với kỹ thuật mã hóa truyền thống, các độ đo để đánh giá hiệu năng bảo mật tầng vật lý trong mạng NOMA.

2. Luận án đề xuất chiến lược bảo mật thông tin cho mạng NOMA cộng tác trên kênh truyền α-μ fading bị thiết bị gây nhiễu và nghe lén hợp tác tấn công dựa trên biểu thức chính xác của phép đo xác suất dừng bảo mật trong kịch bản hệ thống có chiến lược đối phó chủ động và không có chiến lược đối phó chủ động. Các kết quả mô phỏng đã chỉ ra rằng hiệu năng bảo mật của hệ thống được cải thiện đáng kể trong kịch bản có chiến lược đối phó chủ động.

3. Luận án đã đề xuất và đánh giá hiệu năng bảo mật mô hình mạng NOMA có chiến lược chủ động nghe lén. Tác giả đã xây dựng một chính sách điều khiển công suất phát trong kịch bản trạng thái kênh truyền xác định và không xác định vừa đảm bảo hiệu suất nghe lén vừa thỏa mãn ràng buộc về QoS của hệ thống truyền tin bất hợp pháp. Mặt khác, luận án sử dụng độ đo xác suất nghe lén thành công để đánh giá hiệu năng bảo mật của hệ thống và đánh giá hiệu suất nghe lén hợp pháp thành công đối với người dùng bất hợp pháp có tín hiệu mạnh nhất và người dùng bất hợp pháp có tín hiệu yếu nhất. Các kết quả phân tích lý thuyết và mô phỏng chỉ ra rằng hiệu năng bảo mật của hệ thống tăng đáng kể khi số lượng ăng-ten của thiết bị chuyển tiếp tăng lên.

4. Luận án đã nghiên cứu, đánh giá khả năng bảo mật thông tin tầng vật lý mô hình mạng NOMA đơn đầu vào, đơn đầu ra với các kịch

bản khác nhau về thiết bị nghe lén Eve. Hiệu năng bảo mật được phân tích, đánh giá thông qua các độ đo xác suất dừng bảo mật của từng người dùng, của toàn bộ hệ thống với kịch bản Eve sử dụng các kỹ thuật SIC, PIC để xử lý tín hiệu thu được, kịch bản Eve được trang bị một và nhiều ăng-ten. Các kết quả phân tích lý thuyết và mô phỏng đã chỉ ra rằng hiệu năng bảo mật của hệ thống trong trường hợp Eve sử dụng PIC kém hơn so với trường hợp Eve sử dụng kỹ thuật SIC. Hơn nữa, hệ thống sẽ bảo mật hơn khi Eve chỉ được trang bị một ăng-ten so với trường hợp thiết bị nghe lén được trang bị nhiều ăng-ten.

5. Luận án đã phân tích mối quan hệ giữa bảo mật và độ tin cậy trong mạng NOMA nhận thức dạng nền dưới ràng buộc mức can nhiễu của mạng sơ cấp và công suất phát mức đỉnh của mạng thứ cấp, từ đó đưa ra chính sách điều chỉnh công suất phát của mạng thứ cấp để vừa đảm bảo khả năng bảo mật của mạng thứ cấp và QoS của mạng sơ cấp. Các kết quả đã chỉ ra rằng giữa bảo mật và độ tin cậy có mối quan hệ tỷ lệ nghịch. Hiệu năng bảo mật của mạng thứ cấp được cải thiện khi giảm công suất phát và khi số lượng cặp người dùng của mạng sơ cấp tăng thì có thể giảm công suất phát của mạng thứ cấp.

DANH MỤC CÔNG TRÌNH KHOA HỌC CỦA TÁC GIẢ LIÊN QUAN ĐẾN LUẬN ÁN

A. Các công trình khoa học được sử dụng trong luận án

[A1] **Tung Pham Huu**, Van Nhan Vo, Hung Tran and Truong Xuan Quach and Viet Nguyen Dinh, "Secrecy Performance Analysis of Cooperative NOMA Networks With Active Protection under α - μ Fading",*2019 International Conference on Advanced Technologies for Communications (ATC)*, Hanoi, Vietnam, 2019, pp. 215-22.

[A2] **Tung Pham Huu**, Tam Ninh Thi-Thanh, Chi Nguyen-Yen, Hung Tran, Viet Nguyen Dinh and Van Vo Nhan, "Secrecy Outage Probability and Fairness of Packet Transmission Time in a NOMA System",*IEEE Access*, vol. 8, pp.79637-79649, 2020.

[A3] **Tung Pham Huu**, Van Vo Nhan, Hung Tran, Truong Quach Xuan and Viet Nguyen Dinh, "Proactive Eavesdropping via Jamming in NOMA Network", *IEEE Access*, vol. 9, pp.168121-168133, 2021.

[A4] **Tung Pham Huu**, Hung Tran, Duc-Tan Tran, Viet-Hung Dang, Van Nhan Vo, and Viet Nguyen Dinh, "Security and Reliability Performance Analysis of Cognitive NOMA Network Under Outage Constraint of Multiple Primary Users", *12th International Symposium on Information and Communication Technology (SoICT 2023)*, Ho Chi Minh City, Vietnam, 2023.

B. Các công trình khoa học có liên quan đến luận án

[B1] **Tung Pham Huu**, Truong Xuan Quach, Hung Tran, Hans-Jurgen Zepernick, and Louis Sibomana (2017), "On proactive attacks for coping with cooperative attacks in relay networks", *23rd Asia-Pacific Conference on Communications (APCC)*, Perth, 2017, pp. 1-6.

[B2] Van Nhan Vo, Chakchai So-In, Hung Tran, Duc-Dung Tran and **Tung Pham Huu**, "Performance Analysis of an Energy-Harvesting

IoT System Using a UAV Friendly Jammer and NOMA Under Cooperative Attack," in IEEE Access, vol. 8, pp. 221986-222000, 2020.

[B3] Hung Tran, Hung Pham Ngoc, Van Vo Nhan, Xuan Truong Quach, **Tung Pham Huu**, Long Nguyen Quoc, and Giang Quynh Le Vu "Secure Conversation: A View From Physical Layer", *The 12th International Conference on Computational Data and Social Networks*, Hanoi, Vietnam, 2023.

[B4] Hung Tran, **Tung Pham Huu**, Lam-Thanh Tu, Vu Le Quynh Giang, Trinh Van Chien, Viet-Hung Dang, and Vo Nhan Van, "Packet Timeout Probability of CRN under Security Constraints of Multiple Primary Users", *12th International Symposium on Information and Communication Technology (SoICT 2023)*, Ho Chi Minh City, Vietnam, 2023.